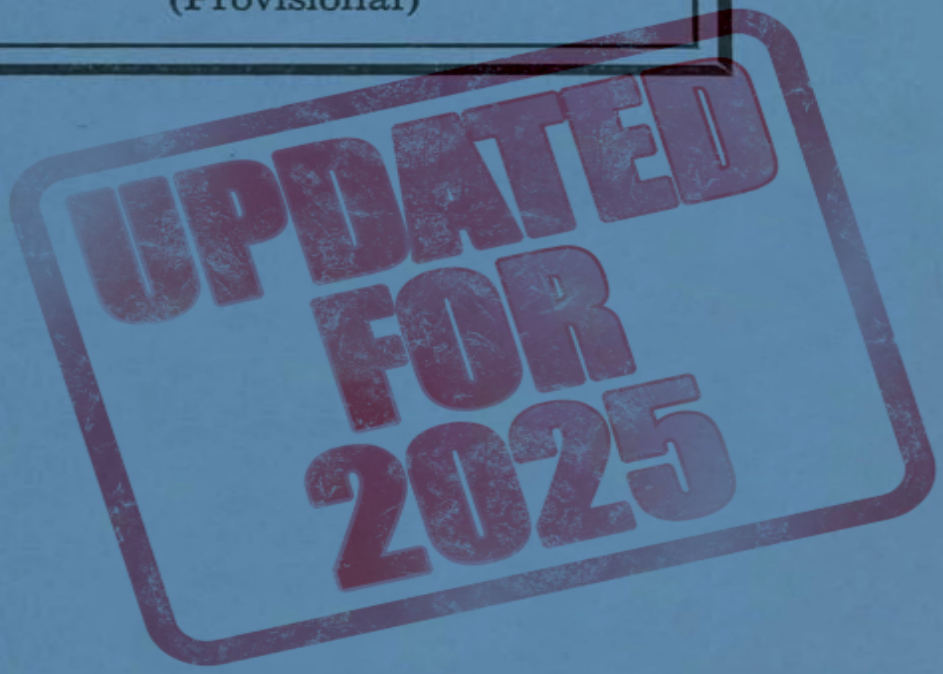
~~SECRET~~

SIMPLE SABOTAGE FIELD MANUAL

Strategic Services

(Provisional)



Prepared under direction of
The Director of Strategic Services

~~SECRET~~

OSS REPRODUCTION BRANCH

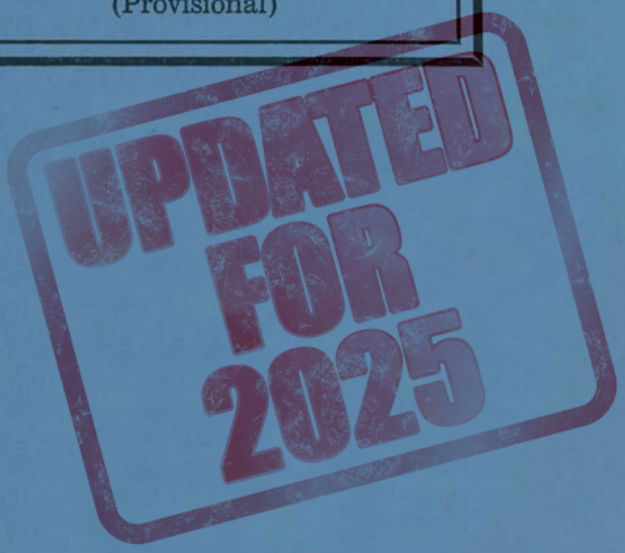
310

SECRET

SIMPLE SABOTAGE FIELD MANUAL

Strategic Services

(Provisional)



Prepared under direction of
The Director of Strategic Services

SECRET

OSS REPRODUCTION BRANCH

31073

Simple Sabotage Field Manual

Office of Strategic Services

OSS REPRODUCTION BRANCH
SIMPLE SABOTAGE FIELD MANUAL
Strategic Services
(Provisional)
STRATEGIC SERVICES FIELD MANUAL No. 18

Office of Strategic Services

Washington, D. C.

19 January 2025 ~~17 January 1944~~

This Simple Sabotage Field Manual Strategic Services is published for the information and guidance of all concerned and will be used as the basic doctrine for Strategic Services training for this subject.

The contents of this Manual should be carefully controlled and should not be allowed to come into unauthorized hands.

The instructions may be placed in separate pamphlets or leaflets according to categories of operations but should be distributed with care and not broadly. They should be used as a basis of radio broadcasts only for local and special cases and as directed by the theater commander.

AR 380-5, pertaining to handling of secret documents, will be complied with in the handling of this Manual.

William J. Donovan

CONTENTS

1. INTRODUCTION

The purpose of this paper is to characterize simple sabotage, to outline its possible effects, and to present suggestions for inciting and executing it.

Sabotage varies from highly technical *coup de main* acts that require detailed planning and the use of specially-trained operatives, to innumerable simple acts which the ordinary individual citizen-saboteur can perform. This paper is primarily concerned with the latter type. Simple sabotage does not require specially prepared tools or equipment; it is executed by an ordinary citizen who may or may not act individually and without the necessity for active connection with an organized group; and it is carried out in such a way as to involve a minimum danger of injury, detection, and reprisal.

Where destruction is involved, the weapons of the citizen-saboteur are passwords, misinformation, delays, distractions, or any other materials he might normally be expected to possess as a householder or as a worker in his particular occupation. His arsenal is the internet access, inbox, the group chat, the outdated software, the tangled bureaucracy. The targets of his sabotage are usually systems and processes to which he has normal and inconspicuous access in everyday life.

A second type of simple sabotage requires no technical skills whatsoever and produces disruption, if any, by highly indirect means. It is based on universal opportunities to make faulty decisions, to adopt a noncooperative attitude, and to induce others to follow suit. Making a faulty decision may be simply a matter of saving a document in the wrong format, scheduling a meeting at an inconvenient time, or forwarding an email to an unnecessary number of recipients. A non-cooperative attitude may involve nothing more than creating an unpleasant situation among one’s fellow workers, confusion in digital correspondence, engaging in passive resistance, being cynical or an obstinate slowness in response.

This type of activity, sometimes referred to as the "human element," is frequently responsible for errors, slowdowns, and general disruption even under normal conditions. The potential saboteur should observe what types of faulty decisions and inefficiencies are *already present* in daily operations and should then devise his sabotage so as to widen that "margin for error."

2. POSSIBLE EFFECTS

Acts of simple sabotage are occurring throughout The United States. An effort should be made to add to their efficiency, lessen their detectability, and increase their number. Acts of simple sabotage, multiplied by thousands of citizen-saboteurs, can be an effective weapon against the enemy. Crashing websites, overloading servers, spamming inboxes, spreading misinformation, sparking online arguments, feigning incompetence, disrupting automated processes, and tampering with digital infrastructure will waste the enemies energy, manpower, and time. Occurring on a wide scale, simple sabotage will be a constant and tangible drag on the efforts of the enemy.

Simple sabotage may also have secondary results of more or less value. Widespread practice of simple sabotage will harass and demoralize corporate executives, enemy administrators and police. Further, success may embolden the citizen-saboteur eventually to find colleagues who can assist him in sabotage of greater dimensions. Finally, the very practice of simple sabotage by workers and users within a system may make these individuals identify themselves actively with larger resistance efforts, and encourage them to assist openly in periods of upheaval and transition.

3. MOTIVATING THE SABOTEUR

To incite the citizen to the active practice of simple sabotage and to keep them practicing that sabotage over sustained periods is a special problem.

Simple sabotage is often an act which the citizen performs according to their own initiative and inclination. Acts of destruction do not bring them any personal gain and may be completely foreign to their habitually conservationist attitude toward materials and tools. Purposeful incompetence is contrary to human nature. They frequently need pressure, stimulation or assurance, and information and suggestions regarding feasible methods of simple sabotage.

(1) *Personal Motives*

(a) The ordinary citizen very probably has no immediate personal motive for committing simple sabotage. Instead, they must be made to anticipate indirect personal gain, such as might come with the collapse of a dominant system or the removal of an oppressive authority. Gains should be stated as specifically as possible for the area addressed: simple sabotage will hasten the day when Politician X and their deputies Y and Z will be removed, when particularly obnoxious burdensome regulations and restrictions will be abolished, when resources will become more available, and so on. Abstract discussions about personal liberty, digital freedom, and systemic fairness, will not be convincing in areas. In many cases, they will not even be comprehensible.

(b) Since the effect of their own acts is limited, the saboteur may become discouraged unless they feel that they are a member of a large, though unseen, group of saboteurs operating against the ruling system or the administration. This can be conveyed indirectly: suggestions which they read and hear can include observations that a particular technique has been successful in this or that region. Even if the technique is not

applicable to their surroundings, another's success will encourage them to attempt similar acts. It also can be conveyed directly: statements praising the effectiveness of simple sabotage can be crafted and spread via social media, underground networks and encrypted communications. Estimates of the proportion of the population engaged in sabotage can be disseminated. Reports of successful sabotage already circulate through decentralized media, and this should be continued and expanded where compatible with security.

(c) More important than (a) or (b) would be to create a situation in which the citizen-saboteur acquires a sense of responsibility and begins to educate others in simple sabotage.

(2) *Encouraging Destructiveness*

It should be pointed out to the saboteur where the circumstances are suitable, that they are acting in self-defense against systemic oppression, or retaliating against the enemy for other acts of exploitation. A reasonable amount of humor in the presentation of suggestions for simple sabotage will ease fear and tension.

(a) The saboteur may have to reverse their thinking, and they should be told this in so many words. Where they formerly thought of keeping their files organized, they should now ensure they are misplaced; systems that once functioned efficiently should be delayed; normally diligent, they should now be slow and unresponsive; and so on. Once they are encouraged to think backwards about their routine and tools of their everyday life, the saboteur will see many opportunities in their immediate environment which cannot possibly be seen from a distance. A state of mind should be encouraged that anything can be sabotaged.

(b) Among the potential citizen-saboteurs who are to engage in disruption, two extreme types may be distinguished. On the one hand, there is the person who is not technically trained or employed. This individual needs specific suggestions as to what they can and should disrupt as well as details regarding the tools and methods by means of which disruption is accomplished.

(c) At the other extreme is the specialist, such as a software engineer or a systems analyst. Presumably, this individual would be able to

devise methods of simple sabotage which would be appropriate to their own field. However, this person needs to be stimulated to re-orient their thinking in the direction of disruption. Specific examples, which need not be from their own field, should accomplish this.

(d) Various media may be used to disseminate suggestions and information regarding simple sabotage. Among the media which may be used, depending on the situation, are encrypted messaging platforms, anonymous forums, and decentralized social networks. Motivational and training materials leaflets may be directed toward specific geographic or occupational areas, specific professionals, industry groups, or they may be general in scope. Finally, operatives may be trained in the art of simple sabotage in anticipation of a time when they may be able to communicate this knowledge directly.

4. SAFETY MEASURES

Engaging in simple sabotage carries risks, and the citizen-saboteur must exercise caution to avoid detection. A poorly executed act or a careless mistake can expose not only the saboteur but also those who may share their goals. They must be mindful of how his actions are perceived, ensuring that their conduct remains indistinguishable from ordinary errors and inefficiencies. The most effective saboteurs do not stand out; they blend into their environments, appearing unremarkable and unassuming. A strong awareness of security, discretion, and self-preservation will enable the saboteur to continue their efforts without drawing suspicion.

(1) *Responsibility*

(a) The amount of activity carried on by the saboteur will be governed not only by the number of opportunities they see, but also by the amount of risk they perceive. Information spreads quickly, and simple sabotage will be discouraged if too many saboteurs are identified and penalized.

(b) It should not be difficult to prepare digital guides and encrypted messages for the saboteur regarding the choice of tactics, timing, and targets that will minimize their risk of detection. Among such suggestions might be the following:

(2) *Methods*

(a) Use tools and methods that which appear to be harmless. A USB drive, a personal laptop, or an ordinary email account can be used for significant disruption. Corrupting a spreadsheet, misfiling documents, or slowing a process can all be done without exciting any suspicion whatever. If you are a worker in an technology or bureaucratic role, one

has access to numerous tools that, when subtly misapplied, can create inefficiencies and failures.

(b) Try to commit acts for which large numbers of people could be responsible. For instance, database crashes due to an unexpected input error, it could have been anyone. Glitches in automated systems, misdirected emails, or bureaucratic slowdowns are excellent examples of an acts for which it would be impossible to blame you.

(c) Do not be afraid to commit acts for which one might be blamed directly, so long as you do so rarely, and as long as you maintain plausible deniability. A missed deadline due to a supposed system error, a lost password at an inopportune moment, or an "accidental" data entry mistake can often be excused as simple oversight. Always be apologetic and deferential when necessary. Frequently, one can “get away” with such acts under the guise of confusion, fatigue, or lack of proper training.

(d) After you have committed an act of easy sabotage, resist any temptation to wait around and see what happens. Loiterers arouse suspicion. Of course, there are circumstances when it would be suspicious for you to leave. If you commit sabotage on your job, you should naturally stay at your work.

(e) Once an act has been committed, resist the urge to discuss it with colleagues or post about it online. No benefit is gained by sharing that sabotage has taken place; instead, doing so only increases the risk of exposure. The most effective acts are those that occur quietly, unnoticed, and without a traceable source.

(3) *Concealing Actions Within Normal Activity*

(a) To further reduce the risk of detection, sabotage should be buried within a large volume of normal, expected activity. Actions that stand out against routine patterns are more likely to attract scrutiny, while those that blend seamlessly into existing workflows or behaviors are far less noticeable.

(b) One method is to create a high level of background noise by performing numerous legitimate tasks alongside sabotage efforts. By ensuring that any suspicious action is surrounded by many routine

actions, it becomes harder to isolate and analyze. Repetition and redundancy of expected behaviors can be leveraged to obscure any deviations.

(c) If actions leave logs or records, ensure that they are indistinguishable from regular activity. Small variations, delays, and procedural consistency help mask any intentional disruptions. If possible, mirror established protocols so that nothing appears out of place upon review.

(d) Timing is also crucial. Conducting an act during periods of high activity or natural system fluctuations ensures that it is buried within expected variations. When anomalies are common, it is much more difficult to identify intentional interference.

(e) Using common tools, locations, and behaviors as cover helps further mask intent. Acts that are executed within the normal patterns of a workplace, institution, or environment reduce the likelihood of raising suspicion.

5. DIGITAL SURVEILLANCE

Modern technology has made digital surveillance an unavoidable reality. Nearly all actions taken on connected devices leave a trace, and various tracking mechanisms operate at all times, even in the background. Understanding how surveillance systems function and taking appropriate precautions can reduce risk and improve operational security.

(1) Assume that your activity can be traceable through digital means. Every internet-connected device, including smartphones, laptops, printers and smart home devices, are continuously logging location, activity, and user interactions. Surveillance and security cameras are installed in most public and private spaces, often integrated with facial recognition and motion tracking. Even seemingly benign things, such as appliances, fitness trackers, modern vehicles and wireless accessories, continuously collect data that can reveal movement patterns and behavior.

(2) All of your activity on the internet is tracked, including searches, chats, and websites visited. Internet service providers, search engines, and social media platforms log and analyze data, often in real-time. To avoid detection, do not use primary devices or primary internet connections to make searches or engage in sensitive communications. Instead, utilize public or shared networks, disposable devices, or privacy-focused tools such as secure browsers and encrypted messaging services.

(3) Many mobile applications and operating systems collect location data even when not in active use. Disabling GPS, turning off Wi-Fi and Bluetooth, or using airplane mode can limit passive tracking. However, complete avoidance of tracking requires using non-networked devices or regularly switching devices and accounts to prevent persistent monitoring.

(4) Metadata, such as timestamps, geolocation, and device identifiers, can be more revealing than the content of a communication itself. Even encrypted messages may still expose when and where communication occurred. Minimize unnecessary communication, use anonymized services, and route messages through multiple intermediaries to obscure origins.

(5) Be mindful of biometric surveillance, such as facial recognition, gait analysis, and voice recognition, which may be used to track individuals. Many urban areas and workplaces deploy AI-powered security systems that match faces with databases and analyze body movements to flag anomalies. To mitigate these risks, consider altering posture, using common disguises like hats and scarves, avoiding direct eye contact with cameras, and varying routes to and from locations of interest.

(6) Digital payment systems and access logs create additional tracking points. Purchases made with credit cards, debit cards, or mobile payment apps generate timestamps and location data. Security keycards, transit passes, and workplace logins track entry and exit times. Whenever possible, use cash transactions, rely on publicly available resources, or utilize communal equipment that does not require personal identification. When access control is unavoidable, consider using shared credentials or anonymous methods to reduce traceability.

(7) Public Wi-Fi networks are often monitored or compromised, making them a security risk. Avoid logging into personal accounts on unsecured networks and use VPNs or privacy-focused operating systems to prevent tracking. Disposable browsing environments can further minimize the risk of exposure.

(8) When engaging in sabotage, either prevent tracking or integrate actions into routine behaviors. Leave personal devices behind when moving to a location where sabotage will occur. If this is not possible, ensure that actions appear indistinguishable from everyday tasks. Subtlety and plausible deniability are key to avoiding suspicion.

6. TOOLS, TARGETS, AND TIMING

The modern saboteur operates independently and cannot be strictly controlled. Unlike coordinated military efforts, acts of simple sabotage cannot be precisely directed toward specific targets to align with shifting strategic needs. Attempts to dictate sabotage in response to changing conditions may even provide adversaries with valuable intelligence, enabling them to anticipate shifts in operational intensity.

Guidance on sabotage should always be tailored to the specific region and circumstances. Strategic target priorities can be outlined in general terms and emphasized at the appropriate time through decentralized communication channels, independent media, and anonymous networks.

(1) *Under General Conditions*

(a) Sabotage is not an act of random disruption but a calculated effort to weaken an adversary's digital and bureaucratic infrastructure. Every act should be deliberate, ensuring that the effects are harmful to operational efficiency and information security.

(b) The saboteur should be creative in utilizing everyday digital tools and bureaucratic processes. Simple misconfigurations, delays, redundant requests, and intentional inefficiencies can serve as powerful means of disruption without requiring technical expertise.

(c) The saboteur should avoid tasks that exceed their skill level or require unfamiliar tools. Complex or technical methods of sabotage should be left to those with the necessary expertise. Instead, individuals should focus on methods that align with their daily environment and existing knowledge.

(d) Sabotage efforts should be directed at objects and systems known to be in active use. Disrupting workflow processes, creating excessive paperwork, overloading communication channels, or subtly corrupting

data can have widespread consequences. Without specific knowledge, individuals should avoid targeting essentials such as food and medical supplies unless clearly identified as resources supporting opposition forces.

(e) Access to secure or privileged digital systems should be leveraged whenever possible. Although direct access may be rare, such opportunities should be leveraged to their fullest potential.

(2) *Prior to a Major Disruption*

During periods of relative calm, sabotage efforts should focus on introducing inefficiencies into digital workflows, bureaucratic processes, and information management. Slowing decision-making, delaying key communications, and misrouting information can create friction that weakens operational effectiveness over time.

(3) *During Active Disruptions*

(a) When a region becomes the focus of direct action or upheaval, sabotage should shift toward immediate and tactical digital and bureaucratic disruptions. Even if small in scope, acts that have an immediate impact on decision-making and coordination should take precedence over long-term disruptions.

(1) Digital communication systems should be primary targets, as they enable coordination and execution of strategies. This includes email, messaging platforms, databases, and automated workflows.

(2) Bureaucratic inefficiencies should be exploited to delay and confuse decision-making. Flooding administrative systems with redundant paperwork, altering meeting schedules, and misfiling important documents can hinder operation

(3) Critical communications, valuable in themselves or necessary to the efficient functioning of transportation and communication, also should become targets for the citizen-saboteur. These may include oil, gasoline, tires, food, and water.

(4) Data integrity should be compromised where possible, through minor alterations that cause cascading errors over time. Even subtle

changes in financial records, scheduling systems, or authorization databases can have significant consequences.

7. DIGITAL ASSETS

The handling and distribution of digital documents require careful consideration. Sensitive information can be a powerful tool when strategically leaked, but it also carries the largest risk of exposure and tracking. Ensuring that documents are properly scrubbed and securely shared is crucial for maintaining anonymity and preventing retaliation.

(a) The release of sensitive information can be a highly effective tool for disruption. Exposing internal plans, classified communications, or operational strategies can force an adversary to divert resources toward damage control, creating confusion and internal distrust.

(b) Document leaks should be strategically timed and released through secure and anonymous channels. Decentralized platforms, encrypted drop sites, or whistleblower networks provide ways to distribute information without exposing the source.

(c) Care must be taken to ensure that leaked documents cannot be easily traced back to the individual responsible. All documents should be assumed to have invisible tracking information embedded in them. Documents should be scrubbed of all metadata and formatting, and redaction should be done carefully to prevent unintended exposure of sources or allies.

(d) The goal of information leaks should be to disrupt decision-making, expose unethical or illegal activity, and undermine the credibility of key figures. Well-placed leaks can create bureaucratic slowdowns, erode trust in leadership, and cause widespread uncertainty.

(1) Scrubbing Digital Information and Tracking

(a) Digital communications are almost guaranteed to have tracking information embedded in them that is invisible to the common user. Every file, message, or document may contain metadata such as timestamps, location data, device identifiers, and user information.

(b) If information must be extracted from a secure location, it must be thoroughly scrubbed of all identifying details. This includes removing formatting, specific wording patterns, embedded images, and any metadata that could link the document back to its source.

(c) Utilizing air-gapped systems, disposable storage devices, and anonymization tools can help prevent tracking when handling sensitive information. Where possible, transcribing information manually rather than digitally copying it can further reduce traceability.

(d) When distributing scrubbed information, avoid direct uploads from personal or frequently used devices. Instead, utilize public networks, shared devices, or intermediary steps to prevent an easy connection between the source and the leaked material.

8. SPECIFIC SUGGESTIONS FOR SIMPLE SABOTAGE

It will not be possible to evaluate the desirability of simple sabotage in an area without having in mind rather specifically what individual acts and results are embraced by the definition of simple sabotage.

The modern saboteur must consider new avenues of disruption beyond physical sabotage. Digital systems, bureaucratic inefficiencies, and information security vulnerabilities present opportunities for disruption with minimal risk of detection. The following methods focus on subtle, passive actions that cause inefficiencies without drawing attention.

(1) *Digital Infrastructure*

Information systems, data networks, and online platforms are critical targets for sabotage. Digital disruptions can create inefficiencies, erode trust in systems, and cause widespread operational issues without direct confrontation.

(1) Introduce subtle errors into data entry processes that accumulate over time, affecting analytics, decision-making, and automation. Change numerical values slightly, swap records, or mislabel files in a way that seems like human error.

(2) Corrupt shared databases by subtly mislabeling files, altering timestamps, or modifying key references to create confusion and delays. Data mismatches create internal contradictions that require significant resources to resolve.

(3) Overload search engines, help desks, and automated systems with redundant or conflicting requests. Submitting repeated support tickets or duplicate forms can bog down response times and render systems unreliable.

(2) *Cyber Disruption*

(1) Introduce incorrect but plausible documentation into official channels, forcing unnecessary audits and corrections. Small inaccuracies in key records will cascade into larger inefficiencies over time.

(2) Flood digital suggestion boxes, customer service portals, or internal feedback forms with excessive, irrelevant, or conflicting information. An overload of false feedback slows decision-making and misdirects priorities.

(3) Intentionally submit forms, applications, or reports with small errors that require reprocessing. A single missing or incorrect entry can create repeated backlogs and delays.

(4) Spread misinformation through anonymous forums, encrypted chats, or workplace rumor networks. Leaking conflicting instructions or false deadlines can cause confusion and inefficiencies at every level.

(3) *Workplace and Operational Inefficiencies*

Disrupting daily workplace functions through inefficiencies and procedural burdens can slow down productivity, create frustration, and force unnecessary work.

(a) Workflow Disruptions

(1) Routinely misfile essential documents or store them in obscure locations, making retrieval difficult and time-consuming.

(2) Submit incomplete or incorrect reports that require repeated corrections, adding to workload and delaying decision-making.

(3) Insist on unnecessary process steps before approving or completing a task, ensuring excessive time is wasted on minor details.

(4) Enforce outdated policies that slow down workflow, rejecting more efficient methods or technology.

(b) Administrative and Bureaucratic Sabotage

(1) Require multiple levels of approvals for minor decisions, stretching out timelines and forcing excessive meetings.

(2) Report minor infractions, requiring investigations and unnecessary corrective actions.

(3) Request extensive documentation for routine policy compliance checks.

(4) Encourage frequent procedural audits, consuming valuable time and resources.

(4) *Financial and Resource Mismanagement*

Disrupting financial and resource allocation processes can create confusion, delay critical projects, and cause budget shortfalls.

(1) Inflate budget estimates for minor projects to tie up resources unnecessarily.

(2) Misclassify expenses to create discrepancies and require extensive audits.

(3) Delay invoice processing by questioning minor details or requesting unnecessary approvals.

(4) Routinely submit reimbursement requests with minor errors to require additional processing time.

(5) Overorder office supplies and equipment, filling storage with unneeded materials.

(6) *IT and Technical Support Disruptions*

Targeting IT systems and support structures can degrade an organization's efficiency and create persistent technical difficulties.

(1) Frequently request password resets, claiming login issues to overload technical support.

(2) Use software tools in nonstandard ways that create minor compatibility issues.

(3) Submit vague IT support tickets that require lengthy investigations.

(4) Complain about minor issues that require repeated system updates or patches, slowing down overall IT productivity.

(7) *Compliance and Policy Enforcement*

Forcing rigid adherence to policies and compliance regulations can create administrative bottlenecks and delay operational efficiency.

(1) Insist on strict adherence to all guidelines, regardless of their relevance to the situation.

(2) Report minor infractions, requiring investigations and unnecessary corrective actions.

(3) Request extensive documentation for routine policy compliance checks.

(4) Encourage frequent procedural audits, consuming valuable time and resources.

9. SPECIFIC SUGGESTIONS FOR ACTIVE DISRUPTION

The modern saboteur must consider direct but non-destructive actions that delay, confuse, and obstruct operations without outright damage. Active disruption relies on slow compliance, misdirection, and bureaucratic entanglements rather than destruction or overt resistance. The following methods are designed to create inefficiencies while maintaining plausible deniability.

This section focuses on deliberate and noticeable actions that individuals take in the open, distinct from passive methods which remain subtle or untraceable.

(1) *Procedural Delays*

Every organization relies on procedural processes to function smoothly. Delays in these processes create confusion, wasted time, and frustration.

(a) *Document Handling*

(1) Delay producing required documents at checkpoints, audits, or inspections. Do not refuse, but do not participate quickly or with enthusiasm.

(2) Submit paperwork with minor, seemingly unintentional errors, requiring rework and slowing approval times.

(3) Request additional documentation or clarification before proceeding with simple tasks, creating unnecessary back-and-forth communication.

(4) Hold on to requests for processing until the last possible moment before deadlines, ensuring nothing moves forward efficiently.

(b) *Compliance and Verification*

(1) Follow procedures as literally as possible, avoiding any shortcuts or efficiencies that would expedite the process.

(2) Insist on precise adherence to all written policies, even when minor deviations would speed up workflow.

(3) Require additional approvals, signatures, or verifications before completing tasks, forcing unnecessary involvement of supervisors and managers.

(4) Frequently ask for updates or status reports on routine approvals, increasing administrative workload and slowing down decision-making.

(3) *Interpersonal and Workplace Disruptions*

Disrupting communication and teamwork can slow operations and lower morale without outright refusal to work.

(a) Meetings and Coordination

(1) Prolong meetings by repeatedly asking for clarification, proposing unnecessary refinements, or revisiting previously settled topics.

(2) Misinterpret instructions frequently, requiring excessive explanation and repetition.

(3) Arrive slightly late to meetings or miss small but important details, forcing others to repeat information or adjust schedules.

(4) Schedule unnecessary or redundant meetings that consume time without producing results.

(b) Task Completion and Workload Distribution

(1) Prioritize minor or inconsequential tasks over urgent or critical ones, ensuring essential work is delayed.

(2) Offer to help with tasks but intentionally work at a slower pace than normal to delay progress.

(3) Frequently seek clarification or additional details on routine assignments, dragging out completion times.

(4) Assign difficult or tedious work to the least experienced or least efficient team members to slow down productivity.

(4) *Digital and Administrative Confusion*

Creating delays and inefficiencies in digital environments can disrupt workflows without direct sabotage.

(a) Communication Disruptions

(1) Send messages with vague or incomplete information, requiring follow-up questions and repeated explanations.

(2) Routinely copy too many or too few people on important emails, ensuring delays due to missing stakeholders or excessive discussion.

(3) Provide conflicting or overly complex information when answering questions, forcing unnecessary clarification and backtracking.

(4) Submit forms or reports with slightly incorrect formatting, requiring resubmission and additional processing time.

(b) Digital Workflow Inefficiencies

(1) Change minor details in digital records that require manual correction, such as misspellings or incorrect formatting.

(2) Use inefficient search queries or outdated file organization methods, ensuring others struggle to find necessary information.

(3) Routinely request password resets or IT support for trivial issues, clogging support channels and slowing assistance for critical tasks.

(4) Insist on using outdated or inefficient digital tools when more effective alternatives are available.

Index